SECTION XI. PHYSICAL SECURITY

87. General. COMSEC material may require different levels of physical security under different conditions. TOP SECRET keying material is our nation's most sensitive keying material, since it is used to protect the most sensitive U.S. national security information and its loss to an adversary can subject to compromise all of the information protected by the key. For this reason, TOP SECRET keying material is afforded the special protection of two-person integrity (TPI)/no-lone zone (NLZ) controls. Any violation of the TPI/NLZ requirements specified herein is reportable as an insecurity in accordance with Section XVI., Paragraph 113.c. Waivers to the requirements for the control of TOP SECRET keying material may be requested; however, maintenance of a strong national COMSEC posture dictates that such waivers be granted on a case-by-case basis only when a genuine hardship exists. Where NSA is the COR, written requests for waivers should be directed through the Contracting Officer's Technical Representative (COTR) to Director, NSA, ATTN: S042 . For contractors who are supported by another COR, requests for waivers should be directed through the appropriate COTR to the COMSEC authority of the user agency involved. The required physical controls pertinent to the specific circumstances are outlined in this Section.

88. Closed Area Designation and Access Controls.

a. A contractor must establish a Closed Area as prescribed in Section IV of the ISM, when the following conditions exist:

(1) There is a contractual requirement to design, analyze, fabricate, test or repair classified cryptographic systems; or to manufacture and/or work on keying materials designated CRYPTO. If the keying material is TOP SECRET, the required no-lone zone controls must also be instituted. These areas must be physically separated from other classified and unclassified project areas. 1/

(2) Open storage of classified COMSEC material is required due to its size or volume.

(3) Operational classified crypto-equipment is keyed and unattended.

(4) Operational CCI crypto-equipment is keyed with classified key and unattended.

NOTE : Where the operational classified or CCI equipment is contained within a special NSA-certified Class 5 security cabinet modified for such application (Such containers may be identified by labels placed in prominent positions inside the containers stating "Modified GSA-Approved Class 5 Security

---

1/ When it is essential in the performance of a contract to remove temporarily such material from a Closed Area, the material must be kept under the constant surveillance of an authorized person who is in a physical position to exercise direct security control over the material. The material must be returned to the controlled area prior to the close of business.

Container certified by NSA for the secure storage/closed-door operation of COMSEC equipment.”) the unit need not be housed in a closed area, provided the supplemental controls specified in Section IV of the ISM are adhered to and the operational keying material in use is classified SECRET or below.

b. In addition to the above, the following requirements with respect to a Closed Area must be observed:

(1) The entrance must be arranged such that persons seeking entry can be identified and prevented from viewing the activities within the area before being permitted to enter.

(2) The door leading to the area must have a sign on the outside designating it a “Closed Area”, but there shall be no indication that COMSEC activities are conducted therein. A security checklist will be placed on the inside of the door showing the date, time and name of the person who unlocked, locked and checked the area. During nonworking hours, the area must be protected as required in paragraph 34a(3) of “the ISM.

(3) During working hours, entrance to the area must be controlled as prescribed in the ISM. When guards are used to control admittance, they must possess an appropriate security clearance and will be given a COMSEC briefing if access as set forth below is involved.

(4) An access list, authenticated by the Facility Security Officer, COMSEC Custodian or Alternate COMSEC Custodian must be prepared and conspicuously displayed within and near the entrance to the Closed Area. The list will indicate with an asterisk or other easily identifiable means, the names of the responsible persons designated to authorize escorted entry of other contractor personnel or authorized visitors. If guards are used during working hours to supervise admittance, the list may be held by the guard controlling entrance to the area.

(5) Avisitor’s register must be maintained inside the area. All persons other than those named on the access list will be required to identify themselves and register when entering and leaving the area. All classified COMSEC material will be concealed from view when visual access is a factor. Visitors permitted in the area will be escorted by an authorized and appropriately cleared person at all times while in the controlled area.

(6) The contractor must not permit the following devices within a Closed Area, unless the use of such devices is required in contract performance:

(a) Cameras, photographic devices/equipment capable of receiving and recording intelligible images.

(b) Sound recording devices/equipments, including magnetic tapes or magnetic wire.

(c) Amplifiers and speakers

(d) Radio transmitting and receiving equipment.

(e) Microphones.

(f) Television receivers.

89. CCI Access Controls.

a. CCI equipment is by definition unclassified, but controlled. Minimum controls for CCI equipment are prescribed under three different conditions: unkeyed, keyed with unclassified key, and keyed with classified key. The provisions apply to CCI equipment which is installed for operational use. Storage requirements for uninstalled CCI equipment are covered in paragraph 90.

(1) Installed and unkeyed: The CCI equipment must be treated as high value property. The contractor is responsible for providing procedural and/or physical controls adequate to prevent unauthorized removal of the CCI equipment or its CCI components. Where it is practical, rooms containing unkeyed CCI equipment should be locked at the end of the work day.

(2) Installed and keyed with unclassified key:

(a) Attended: The contractor is responsible for preventing access by unauthorized personnel through the use of physical controls and/or monitoring access with authorized personnel.

(b) Unattended: The contractor is responsible for preventing access by unauthorized personnel through the use of adequate physical controls (e.g. , locked rooms, alarms, or random checks, etc.).

(3) Installed and keyed with classified key:

(a) Attended: CCI equipment must be under the continuous positive control of contractor personnel who possess a security clearance at least equal to the classification level of the keying material in use, and, if the keying material is TOP SECRET, the NLZ controls must be instituted. User locations where equipment holds TOP SECRET key in key-card form or has mechanical permuters will be operated as no-lone zones (i.e., space in which at least two appropriately cleared individuals must be present). However, NSA has approved a double-padlock hasp which can be installed on card readers or the KW-7 cabinet face to obviate NLZ manning for such locations. No-lone zones are not required when the key is resident in the crypto-equipment in electronic form, or where the crypto-equipment has been modified to preclude access by a lone individual to the hard copy key contained therein. However, two-person integrity controls shall always apply to initial keying and rekeying operations.

(b) Unattended: CCI equipment must be in a Closed Area (refer to paragraph 88, above).

90. STORAGE REQUIREMENTS: A contractor will not be eligible to receive or generate classified COMSEC information until adequate storage has been established at the facility. Storage of TOP SECRET key must meet the requirements of paragraph 90b(1), below.

a. Classified COMSEC Equipment and Information. Classified COMSEC equipment and information other than keying material marked CRYPTO must be stored as prescribed in the ISM for other classified material at the same classification level.

b. Keying Material Marked CRYPTO. Secure storage for keying material marked CRYPTO must be as follows:

(1) TOP SECRET keying material must be stored under two-person (TPI) controls employing two different approved combination locks, with no one person authorized access to both combinations. Storage can be in a special access control container(s) (SACC) which is secured inside a GSA-Approved security container; in a GSA-Approved security container within a Class A vault as prescribed in the ISM or a modular vault composed of panels constructed and certified in accordance with UL standard 608 (M rating or higher); or in a GSA-Approved security container with two built-in combination locks on the master drawer. At least one of the combination locks must be built-in, as in a vault door or in a security container drawer. In addition, supplemental controls as outlined in paragraph 14a(2), ISM, are required.

(2) SECRET keying material may be stored in the same manner as TOP SECRET keying material; or in a steel security file cabinet originally procured from the GSA Federal Supply Schedule; or a Class B vault as prescribed in the ISM. In addition, supplemental controls as outlined in paragraph 14a(4), ISM, are required.

(3) CONFIDENTIAL keying material may be stored in the same manner as TOP SECRET or SECRET keying material; or in a file cabinet having an integral automatic locking mechanism and a built-in, three position, dial type, changeable combination lock; or in a Class C vault as prescribed in the ISM. However, CONFIDENTIAL keying material may be stored in a steel file cabinet equipped with a steel bar and a three-position, dial-type, changeable combination padlock provided the supplemental controls as outlined in paragraph 14a(4), ISM, are in effect.

(4) UNCLASSIFIED keying material may be stored in the same manner as TOP SECRET, SECRET, or CONFIDENTIAL keying material; or in the most secure manner available to the user.

In those exceptional cases when the nature, size, or unique characteristics of the material make it impractical to store as above, the contractor shall safeguard it by control of the area as outlined in paragraph 88, above.

c. CCI Equipment. CCI equipment must never be stored in a keyed condition. Prior to placing CCI equipment in storage, all keying material must be removed, and internal key storage registers zeroized. When unkeyed, CCI equipment must be protected against unauthorized removal or theft during storage (e.g., placed in a locked room, or a room with an adequate alarm system).

91. Record of Individuals Having Knowledge of the Combinations to Containers Storing Classified COMSEC Material. A record must be maintained of the names, addresses, and home telephone numbers of persons having knowledge of

the combination to containers in which classified COMSEC material is stored. In the event of an emergency; e.g., the container or vault is found open after normal working hours, the container must be kept under surveillance and at least one of these individuals will be notified immediately. Normally these containers are under the direct control of the COMSEC Custodian and Alternate COMSEC Custodian; however, where operational need necessitates, classified COMSEC material - to include one edition of current keying material marked CRYPTO - may be issued to a user. Under these circumstances, the notified individual must also contact either the COMSEC Custodian or Alternate COMSEC Custodian. Upon arrival of the summoned individual(s), an inventory of the contents of the container will be immediately undertaken. Upon completion of the inventory, the container combination must be changed and the container locked. The COMSEC Custodian/Alternate COMSEC Custodian will then compare the results of the inventory against the account's COMSEC Register File and, if any material is determined to be missing, this information will be included in the report made in accordance with the provisions of Section XVI.